정 보 보 호 학 회 지
제 32 권 제6호, 2022. 12

모바일 인스턴트 메신저에 대한 TMTO 및 GAN 모델을 활용한 안전성 분석

백 승 준*, 전 용 진*, 허 욱*, 김 종 성**

요 약

모바일 인스턴트 메신저에 적용된 암호기술은 사용자들의 개인정보를 보호하는 역할을 한다. 메신저에 저장된 사용자의 개인정보는 일반적으로 사용자의 패스워드, 사용자 정보 및 기기 정보 기반으로 생성된 암호화 키를 통해 암호화되므로 높은 안전성을 갖는다. 이러한 암호기술의 특성 때문에 국가 법집행기관은 범죄단서 확보 및 사실 증명을 위한 증거 분석과정에 어려움을 겪는다. 그러나, 최근 모바일 인스턴트 메신저를 통해 발생하고 있는 일련의 범죄 사건들을 볼 때 정당한 접근 하에 범죄단서 확보를 위한 암호분석 기술은 활발히 연구될 필요가 있다. 본 논문에서는 10종의 모바일 인스턴트 메신저에 대한 TMTO 및 GAN 모델을 활용한 안전성 분석을 제시한다.

Ⅰ. 서 론

디지털 기술 수준과 인터넷 보급률이 늘어남에 따라 2022년 기준으로 전 세계 인구의 83%(약 66억 명) 이상이 스마트폰을 사용하고 있다[1]. 스마트폰의 사용자들은 각종 애플리케이션을 통해 생활의 편의를 얻고 취미를 향유한다. 그중에서도 모바일 인스턴트 메신저(Mobile Instant Messenger)는 없어서는 안 될 의사소통 수단으로 자리 잡았으며, 스마트폰뿐만 아니라 PC로도 인스턴트 메신저를 사용할 수 있도록 개발되고 있다.

모바일 인스턴트 메신저에 적용된 암호기술은 사용자들의 개인정보를 보호하는 역할을 한다. 반면, 국가 법집행기관은 암호기술로 인해 범죄단서 확보 및 사실 증명을 위한 증거 분석과정에 어려움을 겪는다. 2020년의 박사방 사건 등의 사례로 판단해보면 정당한 접근 하에 범죄단서 확보를 위한 암호분석 기술은 반드시 연구될 필요가 있다.

애플리케이션의 사용자가 만든 패스워드는 무작위성이 낮으므로 전사 공격(Brute-force attack)이나 사전 공격(Dictionary attack)에 공격 될 수 있다. 또한, 사용자의 패스워드가 애플리케이션 내에 평문으로 저장될 경우, 개인 정보 유출이나 패스워드 탈취 등의 악용 소지가 있으므로 평문으로 저장되어서는 안된다. 이를 방지하기 위해 키 생성 알고리즘을 이용하여 패스워드를 특정 반복횟수만큼 해싱한 키로 암호화한 데이터를 저장하는 것이 일반적이다. 자주 사용되는 키 생성 알고리즘으로는 PBKDF2 (Password Based Key Derivation Function 2)[2], PBE (Password Based Encryption)[3]와 SCRYPT[4] 등이 있다.

공격자는 여러 가지 전략으로 애플리케이션 사용자의 패스워드 복구를 시도할 수 있다. 전사 공격의 경우, 모든 가능한 키를 사용하여 암호문을 복호화를 해보아야 하며 비현실적인 공격 시간이 소요된다. 이와 반대로 사전 공격은 알려진 평문에 대한 모든 가능한 키와 암호문 쌍을 얻어서 메모리에 저장해야 하므로 공격자에게 매우 큰 규모의 메모리가 필요하다. 이 두 가지 전략의 절충으로서 Hellman은 TMTO (Time-Memory Trade-Off) 공격을 제시하였다[5]. TMTO 공격의 전략은 일정량의 메모리를 사용하는 대신 공격자가 수행할 키 조사 시간을 줄이는 것이다. 한편, 사전 공격을 위해 사용자 패스워드의 패턴을 분석하고 이를 기반으로 사전을 생성하는 전략 또한 존재한다. 패스워드 패턴 분석 및 생성은 Rule base 혹은

이 논문은 2022년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2021-0-00540, GPU /ASIC 기반 암호알고리즘 고속화 설계 및 구현 기술개발)
* 국민대학교 금융정보보안학과 (대학원생, hellosj3@kookmin.ac.kr, idealtop18@kookmin.ac.kr, gjdnr123@kookmin.ac.kr)
** 국민대학교 금융정보보안학과/정보보안암호수학과 (교수, jskim@kookmin.ac.kr)

확률 트리와 같은 기술을 활용할 수 있으며, 최근에는 머신러닝을 활용한 기술이 연구되고 있다. 2021년 Pasquini 등은 경쟁을 통해 배운다는 개념의 인공지능 기술인 GAN (Generative Adversarial Networks) 모델을 패스워드 생성에 이용하였다[6,7]. 그들은 GAN 모델 기반의 PasswordGAN를 이용하여 패스워드를 생성하고 사용자의 패스워드를 추측하는 방법을 제안하였다.

본 논문에서는 모바일 인스턴트 메신저의 안전성을 분석하여 제시한다. 2장에서는 모바일 인스턴트 메신저의 사용자 키를 복구하는 데 사용될 수 있는 공격 기법들을 설명한다. 3장에서는 PC 버전을 포함한 총 10종의 모바일 인스턴트 메신저를 대상으로 TMTO 공격에 대한 안전성 여부를 분석한다. 4장에서는 GAN 모델을 기반으로 한국인을 타겟으로한 패스워드를 생성하는 모델을 생성한 뒤 결과를 확인하였다. 5장에서는 본 논문의 결론을 맺는다.

Ⅱ. 공격 기법

본 장에서는 모바일 인스턴트 메신저의 사용자 패스워드를 복구하는 데 사용될 수 있는 전사 공격, 사전 공격, TMTO 공격과 GAN 모델을 간략히 소개한다. 여기서, T는 공격에 필요한 시간 복잡도, M은 공격에 사용되는 메모리를 의미한다.

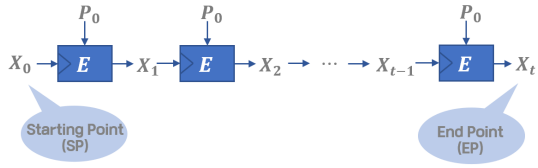
2.1. 전사 공격과 사전 공격

전사 공격은 주어진 평문 및 암호문 쌍에 대하여 모든 가능한 키로 암호문을 복호화 후 복호화된 암호문과 평문의 일치성을 판단하여 실제 키를 찾는 방식이다. 만약 n-비트 키를 추측할 경우 비현실적인 2^n의 복잡도가 소요된다($T=2^n, M\approx 0$). 반면, 사전 공격은 주어진 평문에 대해 모든 경우의 키를 대입하여 키와 암호문 쌍을 얻어 사전에 저장하며, 주어진 암호문과 일치성을 판단하여 실제 키를 찾는 방식이다. 만약 n-비트 키를 추측할 경우 2^n의 메모리가 요구된다 ($T\approx 0, M=2^n$). 사전 공격을 이용하여 키를 복구하기 위해서는 미리 사전을 계산해놓아야 한다는 점과 매우 큰 규모의 메모리가 필요하다는 것이 단점이다.

2.2. TMTO 공격

TMTO 공격은 1980년 Hellman에 의해 제안된 기법으로 전사 공격과 사전 공격의 방법을 절충하는 전략을 취한다[5]. TMTO 공격은 테이블을 미리 선계산하는 오프라인 단계와 주어진 암호문의 암호키를 찾는 온라인 단계로 나뉜다. 사전 계산 테이블을 구성하기 위해 먼저 m개의 균일하게 분포하는 시작점(Starting point)을 정하고, 주어진 평문을 암호화한다. 생성된 암호문은 새로운 키가 되며, 새로운 키로 주어진 평문을 반복해서 암호화한다. 이 과정을 t번 반복한 마지막 암호문을 끝점(End point)으로 정하며, 하나의 체인을 구성할 수 있게 된다. 이러한 체인을 m개 생성하고 각 체인의 시작점과 끝점만을 저장한 것을 Hellman 테이블로 정의한다. Hellman 테이블은 여러 개 구성될 수 있으며, 일반적으로 t개를 구성한다. [그림 1]은 TMTO 키 체인 생성 과정을 보여준다.

암호키를 찾는 온라인 단계에서는 t개의 Hellman 테이블을 고려했을 때, $T=t^2$번의 암호화 연산을 수행해야 하며, 그때 필요한 메모리 크기는 $M=mt$이다. 따라서 대상 키 공간의 크기가 2^n라 가정하면, $O(2^{2n})=M^2T$의 트레이드 오프를 만족하게 된다. $t^2/2$번의 연산으로 전체 테이블 검색이 가능하도록 Rainbow 테이블을 구성할 수도 있다[8].



〔그림 1〕 TMTO 키 체인 생성 과정

2.3. Password Guessing

사용자가 설정한 패스워드는 사용자에 따라 어느 정도 패턴이 존재한다. 대표적인 패턴으로는 숫자 혹은 특수문자가 패스워드의 마지막 부분에서 사용되는 특징이 있다. 또한, 의미 없는 랜덤한 문자열보다는 이름을 포함한 의미 있는 단어들이 사용되고, 숫자의 경우 특정 날짜와 관련된 경우가 많다. 이러한 패턴을 사용하는 대표적인 Password Guessing 도구로는 John the ripper가 존재한다[9]. Jone the ripper는 특정 패턴

을 입력하면 패턴과 일치하는 패스워드를 생성할 수 있다. 그 외에도 Markov 모델과 PCFGs (Probabilistic Context Free Grammars)와 같은 확률 트리 기반의 기법도 활용되고 있다. 최근에는 머신러닝 기술을 활용하여 패스워드를 생성하는 기법이 연구되고 있다 [10,11].

Ⅲ. TMTO 공격 기반 모바일 인스턴트 메신저 안전성 분석

본 장에서는 KakaoTalk, KakaoTalk Channel, Wickr, Wickr(자동로그인), Signal, WeChat, TelegramX와 Private Text Message의 TMTO 공격에 대한 안전성을 분석한다. [표 1]은 각각의 애플리케이션 정보를 제시한 것이며, Salt 값은 키 생성 시 사용되는 추가 데이터이다.

본 논문에서 조사한 메신저들이 사용하는 키 생성 알고리즘은 PBE, SCRYPT, MD5+SHA256과 PBKDF2가 있으며, 고정값을 키로 사용하는 애플리케이션이 2개, KeyStore에 저장된 키를 사용하는 애플리케이션이 1개가 있다. 메시지를 암호화하는 알고리즘에는 AES128-CBC, AES256-CBC, AES128-GCM과 AES256-GCM가 있다. KakaoTalk과 Signal은 암호화에 Salt 값을 사용하지 않으며, 이외의 애플리케이션들은 암호화에 Salt 값을 추가로 사용한다.

키 생성 시 Salt 값을 사용하는 애플리케이션에 대한 TMTO 공격은 사실상 불가능하다. TMTO는 후보가 되는 패스워드에 대한 암호문을 테이블로 미리 저장하는 것으로 공격 시간을 단축한다. 키 생성에 Salt 값을 사용한다면 Salt 값을 사용하는 테이블을 생성해야 하며, 이는 패스워드 공간의 크기를 늘리는 효과를 가져온다. 이에 따라 Salt 값을 사용하지 않는 Signal과 KakaoTalk 외의 애플리케이션에 대한 TMTO 공격 수행은 사실상 불가능하다. 이 중 Signal은 128-비트 크기의 패스워드를 사용하므로, 사전 생성 테이블의 크기가 비현실적으로 커져 TMTO 공격이 불가능하다.

KakaoTalk은 10자리 숫자를 입력인자로 사용하므로 $10^{10} \approx 2^{33.22}$ 크기의 키 공간을 갖는다. Salt 값을 사용하지 않으므로 단순히 키 공간을 전수조사하는 것으로 키를 찾을 수 있다.

본 논문에서는 KakaoTalk PC 버전을 대상으로 TMTO 공격을 진행했다. 공격에는 Rainbow 테이블을

〔표 1〕 모바일 인스턴트 메신저 애플리케이션 정보

애플리케이션	암호화 알고리즘	키 생성 알고리즘	입력 인자	입력인자 복잡도	Salt 사용 여부
KakaoTalk (모바일)	AES256-CBC	PBE	user_id	10자리 숫자	X (고정값 사용)
KakaoTalk (PC)	AES128-CBC	MD5	UserSequence		X (사용자와 기기에 의존)
KakaoTalk Channel (모바일/PC)	AES256-CBC	고정값	“cipher_pw”	-	O
Wickr (모바일/PC)	AES256-GCM	SCRYPT	Passphrase	사용자 입력 (알파벳+숫자+특수문자)	O
Wickr (자동로그인) (모바일)		MD5+SHA256	Android id	64-비트	O
Signal (모바일)	AES128-GCM	KeyStore	-	128-비트	X (128 비트 조사 필요)
WeChat (모바일)	AES256-CBC	MD5	uid, IMEI	20자리 숫자	O
WeChat (PC)		PBKDF2	Wechat_id, serverKey	256-비트	O
TelegramX (모바일)	AES256-CBC	고정값	“cucumber”	-	O
Private Text Message (모바일)	AES128-CBC	PBE	Password	사용자 입력 (알파벳+숫자+특수문자)	O

〔표 2〕 KakaoTalk PC 버전에 대한 TMTO 분석 결과

패스워드 자리 수	테이블 크기	성공 확률	이론적 성공 확률	테이블 생성 시간	테이블 전체 검색 시간	전수 조사 시간
6	1000 x 1000	56.7%	55.58%	0.199s	0.117s	0.207s
	1200 x 1200	70%	66.22%	0.281s	0.171s	
7	3160 x 3160	50%	55.52%	1.898s	1.15s	2.022s
	3500 x 3500	60%	61.55%	2.32s	1.448s	
8	10000 x 10000	40%	55.58%	19.12s	11.503s	20.208s
	12000 x 12000	63.3%	66.20%	27.756s	17.275s	

사용하여 테이블 검색에 필요한 암호화 연산의 수를 줄이고, 성공확률을 높였다. 각 시행은 하나의 테이블에 대해 30개의 랜덤한 패스워드를 공격하고, 그것의 공격 성공확률을 계산한다. 컴퓨터 사양은 11th Gen Intel(R) Core(TM) i7-11700K @ 3.60GHz이고, 메모리는 64GB이다. 코드는 OpenSSL을 임베딩하여 구성되었다. [표 2]는 KakaoTalk PC 버전에 대한 TMTO 공격 수행 결과를 제시한 것이다.

패스워드 공간과 같은 크기의 테이블을 생성하면 이론적으로는 약 55.5%의 확률을 갖는데, [표 2]를 참고하면 실제로도 비슷한 확률을 갖는다는 것을 알 수 있다. 키 공간과 같은 크기의 테이블이 주어졌을 때, 테이블 전체 검색시간은 전수조사 시간보다 약 1.75배 빠르다.

Ⅳ. GAN 모델 기반 한국인 타겟 패스워드 생성 모델 개발

사용자가 입력한 패스워드는 완전히 랜덤하지 않다. 따라서, 가능한 모든 경우의 수를 조사하는 무차별 대입 공격은 랜덤한 값을 사용하는 암호화 키 조사와 달리 쓰일 확률이 희박한 값에 대한 조사과정이 발생한다. 실제 사람이 사용하는 패스워드는 기억하기 쉽도록 문자, 숫자 및 특수문자 영역이 분리되어 나타나며, 의미 있는 단어 혹은 키보드 배열을 따라가는 경향이 있다. 간단한 예시로 ‘v$i1o*e4tr’ 같은 복잡한 패스워드보다 ‘qwert12#’같은 패스워드를 사용할 가능성이 높다. 또한, 사용자의 국적에 따른 차이 또한 존재한다. 예를 들어 영어권 국가에서 ‘iloveyou’를 사용한다면 한국어를 사용하는 국내에선 ‘사랑해’를 키보드로 입력한 ‘tkfkdgo’를 사용한다. 따라서, 효율적인 패스워드 조사를 위해서는 패스워드로 사용되는 값들의 특성과 사용자의 국적 등의 특성을 반영한 값을 조사할 필요가 있다.

본 장에서는 유출된 사용자 패스워드 데이터 세트를 학습하여 패스워드를 생성하는 머신러닝 모델을 소개한다. 또한, 실제 유출 데이터 세트에서 국내 사용자의 패스워드를 추출한 뒤 국내 사용자의 패스워드 특성을 분석하였다. 최종적으로 추출된 국내 사용자의 패스워드를 학습 데이터로 사용한 머신러닝 모델을 개발하였다. 본 장에서 개발된 모델은 [표 1]에 나타난 사용자 입력 패스워드를 사용하는 인스턴트 메신저인 Wickr와 Private Text Message에 활용될 수 있다.

4.1. GAN 모델을 활용한 패스워드 생성

본 논문에서는 패스워드 생성을 위해 오픈소스로 공개된 2021년 발표된 Pasquini의 PasswordGAN을 사용하였다[6,7]. 해당 모델은 학습된 데이터를 기반으로 진짜와 구분하기 힘든 가짜 데이터를 생성하는 GAN 모델을 활용한다. 모델은 랜덤한 값을 생성자에 입력하면 패스워드를 생성하는 방식으로 동작한다.

4.2. 한국인 타겟 생성 모델 개발

본 논문에서 활용한 PasswordGAN 모델을 포함하여 공개된 다양한 패스워드 생성 모델은 대부분 영어권 사용자를 대상으로 개발되었다. 따라서, 본 논문에서는 한국인 사용자를 대상으로 한 패스워드 생성 모델을 개발하였다. 모델 학습에 사용된 데이터는 ‘Exploit.in’으로 불리는 유출된 패스워드 데이터 세트를 활용하였다[12]. 해당 데이터 세트는 2016년에 유출된 것으로 알려졌으며, 593,427,119개의 이메일과 패스워드 쌍으로 구성되어 있다. 이 중 한국인의 계정 정보를 추출하기 위해 naver.com, 및 .kr 등 국내 도메

〔표 3〕 Exploit.in 데이터 세트의 한국 도메인 추출 결과

도메인	추출 결과
naver.com	987,865
hanmail.com	444,706
관공서 (go.kr)	2,333
대학 (ac.kr)	14,842
기타 (.kr)	159,654
합계	1,609,400

인이 사용된 약 160만 개의 이메일과 패스워드를 추출하였고, 결과는 [표 3]에 요약되어 있다.

추출된 계정의 패스워드를 분석한 결과 전체 데이터 세트에서와 달리 'tkfkdgo(사랑해)'와 '1004'등 한국어 사용자에 대한 특성이 반영된 것을 [표 4]에서 확인할 수 있다. 또한, 추출된 데이터를 사용하여 모델을 학습시킨 뒤 실제 패스워드를 생성한 결과 랜덤한 값이 아닌 패스워드의 특성을 반영한 값 위주로 데이터가 생성되는 것을 확인하였다. 또한, [한글]+[숫자]의 패턴을 가지는 값도 다수 확인되었으나 자음과 모음이 제대로 결합 되지 않거나 의미가 불분명한 단어가 주로 생성되었다. 이는 학습데이터가 기존의 0.25% 수준으로 감소한 영향으로 판단된다. Password Guessing 기반의 정량적인 안전성 분석은 불가능하다. 하지만, 패스워드의 특성을 반영한 값의 경우의 수는 가능한 모든 경우에 비해 극히 일부분이므로 일반적인 패스워드 사용 시 안전성이 크게 감소함을 확인할 수 있다.

〔표 4〕 추출된 패스워드 데이터 분석 결과

등장 횟수	패스워드
3516	123456
3063	1234
2901	123123
2070	@!@
1688	tkfkdgo (사랑해)
1541	1q2w3e
1521	1111
988	tkfkdgo1 (사랑해1)
962	123qwe
927	1q2w3e4r
887	qwe123
768	1004
719	asd123

Ⅴ. 결 론

본 논문에서는 모바일 인스턴트 메신저의 안전성을 TMTO와 GAN 모델을 활용하여 분석하였다, TMTO 공격의 경우 Salt 값을 사용하는 애플리케이션에 적용하는 것이 사실상 불가능하나 Salt를 사용하지 않는 애플리케이션에는 적용할 수 있다. 하지만 Salt 값을 사용하지 않더라도 패스워드의 복잡도가 너무 높다면 사전 생성 테이블의 크기가 비현실적으로 커지므로 TMTO 공격을 적용하기 어렵다. 이는 4장에서 제시한 GAN 모델 기반 패스워드 생성 모델로 극복할 수 있다. GAN 모델을 활용하여 만드는 패스워드 후보 집합은 본래 검색해야 하는 패스워드 집합보다 크게 감소한다. 따라서, GAN 모델 기반 패스워드 생성 모델은 독자적으로도 사용될 수 있으며, 향후 TMTO의 사전 생성 테이블을 생성하는 오프라인 단계에도 적용 가능할 것으로 예상된다.

암호기술이 적용된 모바일 인스턴트 메신저가 여러 범죄의 온상이 되고 있으며, 이에 대한 대책 마련이 시급한 상황이다. 본 논문에서 제시한 분석 결과들을 확장하여 국가 법집행기관에서 범죄수사에 필요로 하는 요소기술을 개발하는 것이 필요할 것으로 보인다.

참 고 문 헌

[1] "Bankmycell", https://www.bankmycell.com/blog/how-many-phones-are-in-the-world

[2] M. S. Turan, E. Barker, W. Burr, and L. Chen, "Recommendation for password- based key derivation" *NIST special publication 800*, 2010.

[3] B. Kaliski, "RFC 2898, PKCS 5: Password-Based Cryptography Specification Version 2.0, 2000", Google Scholar Google Scholar Digital Library Digital Library, 2000.

[4] Tarsnap, "http://www.tarsnap.com/scrypt.html"

[5] M. Hellman, "A cryptanalytic time- memory trade-off", *IEEE transactions on Information Theory*, 26(4), pp. 401-406, 1980.

[6] "Improving Password Guessing via Representation Learning", https://github.com/pasquini-dario/PLR

[7] D. Pasquini, A. Gangwal, G. Ateniese, M.

Bernaschi, M. Conti, "Improving password guessing via representation learning", 2021 IEEE Symposium on Security and Privacy (SP). IEEE, 2021.

[8] 김영식, 임대운, “메모리 효율적인 TMTO 암호 해독 기법”. 한국통신학회논문지, Vol.34, No.1, pp. 28-36, 2009.

[9] “John the Ripper password cracker”, https://www.openwall.com/john/

[10] Wikipedia, “Markov chain”, https://en.wikipedia.org/wiki/Markov_chain

[11] Wikipedia, “Probabilistic context-free grammar”, https://en.wikipedia.org/wiki/Probabilistic_context-free_grammar

[12] “EXPLOIT.IN DATA BREACH ANALYSIS”, https://breachdirectory.com/blog/exploit-in-data-breach-analysis/

〈저 자 소 개〉

백 승 준 (Seungjun Baek)

학생회원

2019년 2월 : 국민대학교 수학과 졸업
2022년 2월 : 국민대학교 금융정보보안학과 석사
2022년 3월~현재 국민대학교 금융정보보안학과 박사과정
<관심분야> 정보보호, 암호알고리즘, 디지털 포렌식

전 용 진 (Yongjin Jeon)

학생회원

2018년 8월 : 국민대학교 정보보안암호수학과 졸업
2020년 8월 : 국민대학교 금융정보보안학과 석사
2020년 9월~현재 : 국민대학교 금융정보보안학과 박사과정
<관심분야> 정보보호, 암호알고리즘, 디지털 포렌식

허 욱 (Uk Hur)

학생회원

2019년 2월 : 건국대 신소재공학과 졸업
2021년 2월 : 국민대학교 금융정보보안학과 석사
2021년 3월~현재 : 국민대학교 금융정보보안학과 박사과정
<관심분야> 정보보호, 디지털 포렌식

김 종 성 (Jongsung Kim)

종신회원

2006년 11월 : K.U.Leuven, ESAT/SCD-COSIC 정보보호 공학박사
2007년 2월 : 고려대학교 정보보호대학원 공학박사
2009년 9월~2013년 2월 : 경남대학교 e-비즈니스학과 교수
2013년 9월~2017년 2월 : 국민대학교 수학과 교수
2017년 3월~현재 : 국민대학교 정보보안암호수학과/금융정보보안학과 교수
<관심분야> 정보보호, 암호알고리즘, 디지털 포렌식